SSH-Aufgaben

Name:

Klasse: Datum:

1.1 Lesen Sie die Artikel de.wikipedia.org/wiki/Secure_Shell und de.wikipedia.org/wiki/Public-Key-Authentifizierung! Machen Sie sich strukturierte Notizen, insbesondere zu den Abschnitten Funktionsweise und Sicherheit, sowie zur Public-Key- Authentifizierung!

1.2 Nach erfolgreichem Aufbau der verschlüsselten Verbindung wird ein Sitzungsschlüssel erzeugt, mit dem alle Nutzdaten verschlüsselt werden. Erläutern Sie den Zweck dieses zusätzlichen Schlüssels!

1.3 Erläutern Sie anhand des Artikels de.wikipedia.org/wiki/Tunnel_(Rechnernetz) den Begriff Tunnel!

1.4 Welchen Port nutzt SSH standardmäßig?

1.5 Betrachten Sie das Bildschirmfoto des Programms Putty! Warum ist es ratsam, den Fingerabdruck des Serverschlüssels auf dem Clienten dauerhaft zu speichern?

1.6 Egal ob Sie Putty unter Windows, oder den Linuxkonsolenbefehl SSH starten, der Fingerabdruck wird im Profil des gerade angemeldeten Benutzers und nie im benutzerunabhängigen Teil, z.B. **`HKEY_LOCAL_MACHINE`** bzw. **`/etc/ssh/`** gespeichert. Was ist die Konsequenz?

2.1 Erläutern und interpretieren Sie die Dateiberechtigungen der privaten und öffentlichen Schlüssel im Ordner **`/etc/ssh`**!

2.2 Legen Sie mit den Konsolenbefehlen **`useradd -m sshuser`** und **`passwd sshuser`** ein neues Standardkonto an!

2.3 Starten Sie SSHD und bauen Sie aus der Linuxkonsole mit **`ssh sshuser@localhost`** eine SSH-Verbindung auf!

2.4 Machen Sie einen weiteren Test mit dem Windows-Programm Putty, s. Fundus!

2.5 Machen Sie sich mit der Handhabung des Konsolenbefehls **`scp`** vertraut und erläutern Sie wichtige Parameter!

2.6 Laden Sie die portable Version des Programms WinSCP aus dem Fundus und versuchen Sie mit diesem Programm Dateien zwischen dem Windows-Wirtsrechner und der virtuellen Linux-Machine zu übertragen! Beschreiben Sie Ihre Vorgehensweise!

2.7 Vergleichen Sie die Ausgaben folgender Linux-Kondolenbefehle: **`id, users, whoami`** und **`who -Ha`** und geben Sie jeweils den Verwendungszweck an!

2.8 Finden Sie die Bedeutung aller fett markierten Parameter der Datei **`/etc/ssh/sshd_config`** heraus! Hinweise finden Sie auf der OpenSSH-Manpage.

2.9 Suchen Sie aus der OpenSSH-Manpage die Bedeutung und Handhabung der Konfigurationsparameter **`AllowUsers, DenyUsers, AllowGroups`** und **`DenyGroups`** heraus!

2.10 In welchen Situationen erscheint es sinnvoll, die SSH-Serverschlüssel zu erneuern?

3.1 Laden Sie die Programme Putty, Puttygen und WinSCP aus dem Fundus und setzen Sie PPK-Authentifizierung praktisch um!

3.2 Begründen Sie: Inwiefern ist PPK sicherer als die Anmeldung mit Benutzername und Passwort?

3.3 Dokumentieren Sie jeden Schritt ausführlich!